**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF TEXAS**
**HOUSTON DIVISION**

| | |
|---|---|
| DANIEL JANDRES, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br>v.<br><br>HALLIBURTON COMPANY and HALLIBURTON ENERGY SERVICES, INC.<br><br>Defendants. | Case No. 4:24-cv-03296<br><br>**CLASS ACTION**<br><br>**DEMAND FOR JURY TRIAL** |

# CLASS ACTION COMPLAINT

Plaintiff Daniel Jandres ("Plaintiff"), on behalf of himself and all others similarly situated ("Class Members"), alleges the following against Defendants Halliburton Company and Halliburton Energy Services, Inc. (collectively, "Halliburton"), upon Plaintiff's personal knowledge and upon information and belief, including the investigation of counsel.

## I. INTRODUCTION

1. This action arises from Halliburton's failure to safeguard the personally identifiable information[1] ("PII") and protected health information ("PHI") of Plaintiff and the proposed Class Members, current and former Halliburton employees. Due to Halliburton's deficient data security, the notorious criminal ransomware group known as RansomHub accessed its information technology network and systems and exfiltrated Plaintiff's and Class Members' PHI and PII stored

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

therein, including, on information and belief, their names, dates of birth, Social Security numbers, identification documents, employment files, financial account information, health insurance information, and other medical information (collectively, "Private Information"), causing widespread injury and damages to Plaintiff and Class Members (the "Data Breach").

2. Halliburton is a multinational conglomerate and one of the world's largest companies in the energy, engineering, and defense industries. According its publicly filed quarterly report for the fiscal quarter ended June 30, 2024, Halliburton employs approximately 49,000 employees and has operations in over 70 countries across five continents. Halliburton Company's reported revenue for the three months ended June 30, 2024, exceeded $5.4 billion.

3. Plaintiff and Class Members are current and former Halliburton employees who, as a condition of receiving employment and compensation from Halliburton, were required to and did entrust Halliburton with their sensitive, non-public Private Information. Halliburton collected, used, and maintained Plaintiff's and Class Members' Private Information in order to facilitate its operations, including employment and payroll functions, and stored this Private Information in its network systems.

4. Businesses that handle employees' Private Information like Halliburton owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to the invasion of their private health and financial matters.

5. Halliburton breached its duties owed to Plaintiff and Class Members by failing to

safeguard the Private Information that it collected and maintained, including by failing to implement industry standards for data security to protect the sensitive data against cyberattacks, which allowed a notorious criminal ransomware group to access and steal millions of individuals' Private Information from Halliburton's care.

6. According to Halliburton's regulatory filing about the Data Breach, on August 21, 2024, it "became aware that an unauthorized party had gained access to certain of its systems," specifically, those supporting Halliburton's operational and corporate functions. Halliburton later determined that hackers accessed and exfiltrated files from its systems in the Data Breach.

7. Plaintiff has since learned that RansomHub was behind the Data Breach, stealing the Private Information from Halliburton's systems to hold for ransom and threatening to publish it to the RansomHub dark web leak site if Halliburton does not comply with its ransom demand.

8. Upon information and belief, the mechanism of the RansomHub cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Halliburton, and thus, Halliburton knew failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

9. Despite knowing the risks, Halliburton failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Halliburton's negligent and/or careless acts and omissions and its utter failure to protect Plaintiff's and Class Members' sensitive data.

10. Halliburton breached its duties and obligations by failing in one or more of the following ways: (a) to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (b) to design, implement, and maintain reasonable data retention

policies; (c) to adequately train or oversee staff and service providers regarding data security; (d) to comply with industry-standard data security practices; (e) to warn Plaintiff and Class Members of Halliburton's inadequate data security practices; (f) to encrypt or adequately encrypt the Private Information; (g) to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (i) to utilize widely available software able to detect and prevent this type of attack; (j) and to otherwise secure the Private Information using reasonable and effective data security procedures free of foreseeable vulnerabilities and cyberattack incidents.

11. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information. In providing their Private Information to Halliburton, Plaintiff and Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and security maintained, to use it only for business purposes, and to disclose it only as authorized. Halliburton failed to do so, resulting in the unauthorized disclosure of Plaintiff and Class Members' Private Information in the Data Breach.

12. RansomHub targeted and obtained Plaintiff's and Class Members' Private Information from Halliburton because of the data's value in exploiting and stealing Plaintiff's and Class Members' identities. As a direct and proximate result of Halliburton's inadequate data security and breaches of duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information was accessed by cybercriminals that are now threatening to publish it to an untold number of unauthorized actors. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

13. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to breach ensures that the individual will be at a substantially increased and

certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

14. The risk of identity theft caused by this Data Breach is impending and has materialized, as Plaintiff's and Class Members' Private Information was targeted, accessed, and misused by a notorious cybercriminal group that will almost certainly publish the Private Information to the dark web.

15. As a result of Halliburton's deficient cybersecurity and the consequential Data Breach, Plaintiff and Class Members have suffered and will continue to suffer concrete injuries in fact including, *inter alia*, (a) actual and/or materialized and imminent risk of identity theft and fraud; (b) financial costs incurred due to actual identity theft; (c) lost time and productivity dealing with actual identity theft; (d) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; (i) loss of the benefit of their bargains with Halliburton; and (j) the continued risk to their sensitive Private Information, which remains in Halliburton's possession and subject to further breaches, so long as Halliburton fails to undertake appropriate and adequate measures to protect the confidential data it collects and maintains.

16. To recover for these harms, Plaintiff, on behalf of himself and the Class as defined herein, brings claims for negligence/negligence *per se*, breach of contract, invasion of privacy/intrusion upon seclusion, unjust enrichment, and declaratory relief, to address

Halliburton's inadequate safeguarding of Plaintiff's and Class Members' sensitive Private Information in Halliburton's custody.

17. Plaintiff, on behalf of himself and the Class, seeks compensatory, nominal, statutory, and punitive damages, declaratory judgment, and injunctive relief requiring Halliburton to (a) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (b) implement improved data security practices to reasonably guard against future breaches of Private Information in Halliburton's possession; and (c) provide, at Halliburton's own expense, all impacted Data Breach victims with lifetime credit monitoring and identity theft protection services.

## II. PARTIES

19. Plaintiff Daniel Jandres is a natural person, resident, and citizen of Louisiana. Plaintiff Jandres is a former employee of Halliburton, having worked for Halliburton from 2019 through August of 2024, and upon information and belief is a victim of Halliburton's Data Breach.

20. Defendant Halliburton Company is Delaware corporation with its headquarters and principal place of business at 3000 North Sam Houston Parkway East, Houston, Texas 77302. They may be served through their registered agent Capitol Corporate Services, Inc., 1501 S. Mopac Expressway, Suite 220, Austin, Texas 78746.

21. Defendant Halliburton Energy Services, Inc. ("HES"), Halliburton Company's subsidiary, is a Delaware corporation with its headquarters and principal place of business at 3000 North Sam Houston Parkway East, Houston, Texas 77302. They may be served through their registered agent Capitol Corporate Services, Inc., 1501 S. Mopac Expressway, Suite 220, Austin, Texas 78746.

## III. JURISDICTION AND VENUE

15. This Court has personal jurisdiction over Halliburton Company and HES because both Defendants' principal place of business is in Texas, and because both Defendants engage in substantial and continuous activities and conduct business in this state.

16. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5 million, exclusive of interest and costs, the number of Class Members is over 100, and at least one Class Member is a citizen of a state that is diverse from Halliburton's citizenship, namely, Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

17. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law pursuant to 28 U.S.C. § 1367.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Halliburton Company and HES's respective principal places of business are located in this District, and a substantial part of the events giving rise to this action and Plaintiff's claims occurred in this District.

## IV. FACTUAL ALLEGATIONS

### A. Halliburton Collects and Maintains Private Information and Promises to Protect It.

19. Halliburton is one of the largest energy, engineering, and defense companies in the world, reported revenues exceeding $23 billion in the 2023 fiscal year.

20. According to its most recent quarterly report filed with the United States Securities and Exchange Commission ("SEC"), Halliburton employs over 49,000 individuals in over 70 countries around the globe.

21. Halliburton Company is a publicly traded company and HES's parent. Upon

information and belief, HES manages and oversees Halliburton Company and its subsidiaries' staffing and payroll functions for all United States operations and employment. In this role and to facilitate Halliburton's operational and executive functions, including staffing and payroll, HES collects and maintains employees' Private Information, also sharing it with Halliburton Company.

22. Upon information and belief, when the Data Breach happened the Private Information collected from Halliburton employees, including Plaintiff and Class Members, was maintained and transmitted on cloud-based networks and servers shared between and/or accessible by both HES and Halliburton Company.

23. Plaintiff and Class Members are current and former Halliburton employees who, as a condition of receiving employment and compensation and in order to facilitate Halliburton's operational and executive functions, were required to entrust Halliburton with their sensitive Private Information including their names, identification documents, dates of birth, Social Security numbers, bank account numbers and other financial information, medical information, health insurance information, and other sensitive PII and PHI.

24. At all relevant times, Halliburton knew it was storing and using its networks to store and transmit valuable, sensitive Private Information and that as a result, its systems would be attractive targets for cybercriminals.

25. Halliburton also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the thousands of individuals whose Private Information was compromised, as well as intrusion into their private and sensitive personal matters.

26. Halliburton derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information,

Halliburton could not perform its operations, including staffing, executive, and payroll functions.

27. In exchange for receiving Plaintiff's and Class Members' Private Information, Halliburton promised to safeguard the sensitive, confidential data and to only use it for authorized and legitimate purposes.

28. Halliburton made promises and representations to its employees, including Plaintiff and Class Members, that the Private Information it collected would be kept safe and confidential, the privacy of that information would be maintained, and Halliburton would delete any sensitive information after it was no longer required to maintain it.

29. Halliburton maintains uniform and overarching policies on employee data privacy and security as reflected in its Code of Business Conduct, which applies to all entities in the Halliburton corporate family. Through its Code of Business Conduct, Halliburton acknowledges and assures that employees' PII and PHI, including Social Security numbers, bank account numbers, employment files, insurance information, and medical records, "is confidential and must be protected at all times."[2]

30. Halliburton's Code of Business Conduct further promises and warrants to employees in part as follows:

> **Protecting Personal Information**
>
> Halliburton is committed to maintaining the privacy and security of personal information. Halliburton will collect, transmit, disclose or use personal information only in compliance with local law and only for legitimate business purposes. The Company will only collect the amount of personal information that is needed and will not keep the personal information longer than necessary. Safeguarding personal information about individuals includes maintaining the confidentiality of names, ages, nationalities, bank account information and other personal data as defined in applicable laws.

[2] *See* Code of Business Conduct, Halliburton (Apr. 2024), available at https://cdn.brandfolder.io/EYFW0QO1/as/6nrqq636584rkxgmvcq6wwmx/cobc-english.pdf (last visited September 4, 2024).

> Employees who have access to, or work with, personal information are responsible for handling information appropriately and taking all reasonable steps to preserve its confidentiality. We have adopted security procedures to protect personal data from unauthorized access and use.[3]

31. Halliburton's Code of Business Conduct is provided to all of Halliburton's employees during their employment, including to Plaintiff and Class Members.

32. Additionally, upon information and belief during the application process, all applicants for employment with Halliburton, including Plaintiff and Class Members, received a copy of HES's Privacy Statement,[4] which applies to all HES affiliates and entities in the Halliburton corporate family.

33. The Privacy Statement contains further promises and assurances related to data security for employees' Private Information, including that Halliburton is "strongly committed to protecting your privacy," and is "constantly making changes and upgrades to [its] systems and services in order to better serve you."[5]

34. The Privacy Statement further promises Halliburton employment applicants as follows:

> We implement physical, technical, and organizational security measures designed to safeguard and maintain the integrity and confidentiality of the personal information we process. We evaluate and update these measures on a regular basis. . . . We have put in place appropriate safeguards (such as contractual commitments) in accordance with applicable legal requirements to provide adequate protections for your personal information.[6]

---

[3] *Id.*
[4] *See* Halliburton Privacy Statement (Jan. 2019), available at https://halliburton.recsolu.com/app/collect/form/vQhcn3MF-14gSsrPV9oc2A (last visited Sept. 4, 2024).
[5] *Id.*
[6] *Id.*

35. The Privacy Statement also promises and assures employment applicants that the Private Information Halliburton collects from them will be used only for specific, enumerated purposes related to Halliburton's business or legal obligations—none of which permitted purposes include disclosure to a notorious cybercriminal group, as in this Data Breach.

36. Halliburton's promises to adequately maintain and protect Plaintiff's and Class Members' Private Information demonstrates its understanding that such data's confidentiality and integrity is critical.

37. Plaintiff and Class Members have taken reasonable steps to maintain their Private Information in confidence and privacy. Employees in general value the confidentiality of their Private Information and demand security to safeguard it.

38. Plaintiff and Class Members provided their Private Information to Halliburton with the reasonable expectation and mutual understanding that Halliburton would comply with its obligations to keep such information confidential and secure from unauthorized access.

39. Plaintiff and Class Members relied on Halliburton's sophistication to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

40. Plaintiff and Class Members would not have entrusted their Private Information to Halliburton in the absence of its promises to safeguard that information, including in the manners set forth in Halliburton's Code of Business Conduct and Privacy Statement.

41. Halliburton derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Halliburton could not operate its business or perform the services it provides. Indeed, Halliburton's Privacy Statement acknowledges that not collecting such Private Information would "prevent or

delay the fulfillment" of its contractual obligations.[7]

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Halliburton assumed legal and equitable duties to Plaintiff and Class Members, and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure. Halliburton failed to do so, causing this Data Breach.

**B. Halliburton Failed to Adequately Safeguard Plaintiff's and Class Members' Private Information, causing the Data Breach.**

43. Halliburton collected and maintained its current and former employees' Private Information in its computer information technology systems and networks, including when the Data Breach occurred.

44. The information held by Halliburton at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

45. On August 23, 2024, Halliburton first publicly disclosed the Data Breach through a regulatory filing with the SEC, which contained little information other than that on August 21, 2024, it "became aware that an unauthorized third party gained access to certain of its systems."

46. On September 3, 2024, Halliburton supplemented its earlier disclosure through a second SEC filing about the Data Breach, informing that "the unauthorized third party accessed and exfiltrated information from the Company's systems."

47. According to Halliburton's September 3rd SEC filing, the Data Breach has also "caused disruptions and limitation of access to portions of the Company's business applications supporting aspects of the Company's operations and corporate functions."

48. Halliburton failed to disclose that the RansomHub cybercrime group had claimed

[7] *Id.*

responsibility for the Data Breach, that RansomHub stole Private Information from Halliburton's systems to hold it for ransom, or that RansomHub has threatened to publish the Private Information its dark web leak page if Halliburton does not comply with the ransom demand.

49. Upon information and belief, RansomHub employed double-extortion tactics to carry out the Data Breach, through which the hackers first breached Halliburton's network and exfiltrated Private Information stored in un-encrypted form therein, then encrypted the files on Halliburton's systems once the Private Information had been exfiltrated.

50. RansomHub's *modus operandi* during attacks like this Data Breach is to leave a ransom note during encryption of the target's servers directing the target to contact RansomHub through a unique .onion URL.[8]

51. Upon information and belief, during this Data Breach RansomHub left a ransom note for Halliburton that informs, "Your company Servers are locked and Data has been taken to our servers. This is serious. . . . all of your data is on our servers and we can publish it[.]" The ransom note directed Halliburton to a .onion URL to reach RansomHub.

52. However, according to the Joint Cybersecurity Advisory ("CISA"), while RansomHub commonly demands ransom payments to release PII or PHI stolen from breach targets, as in this Data Breach, "payment does not guarantee victim files will be recovered."[9] Indeed, given the Private Information's substantial value on dark web markets, international cybercriminals like RansomHub have no reason to return stolen Private Information upon a ransom payment when they could continue profiting from it instead.

53. To date, Halliburton has provided no notice or information to individuals whose

---

[8] *See #StopRansomware: RansomHub Ransomware* FED. BUREAU INVESTIGATION, ET AL. (Aug. 29, 2024), available at https://www.cisa.gov/sites/default/files/2024-08/aa24-242a-stopransomware-ransomhub-ransomware_0.pdf (last accessed Sept. 4, 2024)

[9] *Id.*

Private Information was compromised in the Data Breach, nor explained critical facts surrounding the event, like the extent of Private Information involved or that it was accessed by the notorious ransomware organization RansomHub, which has threatened to publish the data on the dark web.

54. Notwithstanding the significant injuries the Data Breach and resulting exposure of their Private Information to a notorious cybercriminal organization has caused, and will continue to cause, Plaintiff and Class Members, Halliburton's September 3, 2024, SEC filing assures that "the incident has not had, and is not reasonably likely to have, a material impact on the Company's financial condition or results of operations." In other words, Halliburton expects to continue business as usual while its employees—Plaintiff and Class Members—are left to shoulder the damages caused by its deficient data security.

55. Halliburton could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' Private Information and training its employees on standard cybersecurity practices.

56. For example, if Halliburton had of implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PII/PHI-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate prolonged malicious activity in Halliburton's network systems without alarm bells going off, including the reconnaissance necessary to identify where Halliburton stored PII/PHI, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Halliburton's system without being caught.

57. Halliburton would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would

have stopped the Data Breach or greatly reduced its impact.

58. Halliburton did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiff's and Class Members' Private Information it collected and maintained, such as encrypting files containing Private Information or deleting Private Information from network systems when it is no longer needed, which caused the theft of that Private Information's unauthorized access and exfiltration in the Data Breach.

59. Additionally, according to the *#StopRansomware: RansomHub Ransomware* whitepaper published by CISA, RansomHub typically gains initial access to a targeted network through common techniques like phishing emails or exploiting known vulnerabilities in internet-facing systems.[10] Phishing is a tactic that uses social engineering to send emails containing malicious attachments to targeted organizations or individuals,[11] and relies on user execution (like opening an email or downloading an attachment) to gain access.[12]

60. CISA recommends rudimentary actions that businesses like Halliburton should take immediately to mitigate cyber threats from RansomHub: (a) installing updates for operating systems, software, and firmware as soon as they are released; (b) requiring phishing-resistant multi-factor authentication ("MFA") (i.e., non-SMS text based) for as many services as possible; and (c) training users to recognize and report phishing attempts.[13]

61. Upon information and belief, Halliburton failed to install updates for operating systems, software, and firmware as soon as they were released. Had Halliburton installed such

---

[10] *Id*.

[11] *See* Phishing, MITRE ATT&CK (March 1, 2024), available at https://attack.mitre.org/versions/v15/techniques/T1566/ (last accessed July 9, 2024).

[12] *See* Phishing, MITRE ATT&CK (April 12, 2024), available at https://attack.mitre.org/versions/v15/techniques/T1204/ (last accessed July 9, 2024).

[13] #StopRansomware: RansomHub Ransomware, CISA (Aug. 29, 2024), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a (last visited Sept. 4, 2024).

updates at its first opportunity as advised, the Data Breach would not have occurred, or would have at least been mitigated.

62. Further, upon information and belief, Halliburton failed to require phishing-resistant MFA where possible or adequately train its employees to recognize and report phishing attempts. Had Halliburton required phishing-resistant MFA, and/or trained its employees on reasonable and basic cybersecurity topics like common phishing techniques or indicators of a potentially malicious event, RansomHub would not have been able to carry out the Data Breach through phishing.

63. As a result of Halliburton's failures, Plaintiff's and Class Members' Private Information was stolen in the Data Breach when criminal RansomHub hackers accessed and acquired files in Halliburton's computer systems storing that sensitive data in unencrypted form.

64. Halliburton's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' Private Information, meaning Halliburton had no effective means in place to detect and prevent attempted cyberattacks.

### C. Halliburton Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses in Possession of Private Information are Particularly Suspectable.

65. Halliburton's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

66. Private Information of the kind accessed in the Data Breach is of great value to cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

67. Private Information can also be used to distinguish, identify, or trace an individual's

identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

68. Data thieves regularly target entities that store PHI and PII like Halliburton due to the highly sensitive information they maintain. Halliburton knew and understood that Plaintiff's and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

69. Cyber-attacks against institutions such as Halliburton are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[14]

70. Cyberattacks by the RansomHub group in particular, as in this Data Breach, have been particularly prevalent in recent months. According to CISA, since February 2024 "RansomHub has encrypted and exfiltrated data from at least 210 victims representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors."[15]

71. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records,

[14] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020 23.pdf (last accessed July 8, 2024).

[15] *See #StopRansomware: RansomHub Ransomware* FED. BUREAU INVESTIGATION, ET AL. (Aug. 29, 2024), available at https://www.cisa.gov/sites/default/files/2024-08/aa24-242a-stopransomware-ransomhub-ransomware_0.pdf (last accessed Sept. 4, 2024).

June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Halliburton knew or, if acting as a reasonable multinational conglomerate and employer, should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

72. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[16]

73. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Halliburton's industry, including Halliburton itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[17]

74. Halliburton's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting entities like Halliburton that collect and store PHI.

75. Entities in custody of PHI, like Halliburton, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[18] Indeed, when compromised, healthcare related data is among the most sensitive and personally

---

[16] *See* Identity Theft Resource Center, *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[17] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed July 8, 2024).

[18] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, ITRC (Jan. 2023) https://www.idtheftcenter.org/publication/2022-data-breach-report.

consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[19] Almost fifty percent of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy.[20]

76. Thus, PHI has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[21]

77. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[22] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[23]

78. As an employer in possession of its employees' Private Information, Halliburton

---

[19] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[20] *Id.*
[21] *9 reasons why healthcare is the biggest target for cyberattacks*, SECURESWIVEL, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks (last accessed July 8, 2024).
[22] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows* (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.
[23] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world* (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, Halliburton failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

79. Despite the prevalence of public announcements of data breach and data security compromises, Halliburton failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from being compromised in this Data Breach.

80. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, including RansomHub specifically, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

81. Halliburton was, or should have been, fully aware of the unique type and the significant volume of data on Halliburton's server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

82. Plaintiff and Class Members were the foreseeable and probable victims of Halliburton's inadequate security practices and procedures. Halliburton knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that data.

83. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

**D. Halliburton is Required, But Failed to Comply with FTC Rules and Guidance.**

84. The Federal Trade Commission ("FTC") has promulgated numerous guides that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

85. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Halliburton. These guidelines note that businesses should protect the Private Information that they keep; properly dispose of Private Information that is no longer needed; encrypt Private Information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[24]

86. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25]

87. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented

[24] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).
[25] *Id.*

reasonable security measures.

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures business like Halliburton must undertake to meet their data security obligations.

89. Such FTC enforcement actions include those against businesses like Halliburton. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

90. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Halliburton of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Halliburton's duty in this regard.

91. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[26]

[26] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

92. Halliburton failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

93. Halliburton's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

**E. Halliburton Failed to Comply with Industry Standards.**

94. A number of published industry and national best practices are widely used as a go-to resource when developing an institution's cybersecurity standards.

95. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[27]

96. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

[27] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

97. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[28]

98. Upon information and belief, Halliburton failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST

[28] CISA, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 8, 2024).

Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

**F. Halliburton Owed Plaintiff and Class Members a Common Law Duty to Safeguard their Private Information.**

99. In addition to its obligations under federal and state laws, Halliburton owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Halliburton's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

100. Halliburton owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

101. Halliburton owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

102. Halliburton owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

103. Halliburton owed a duty to Plaintiff and Class Members to disclose in a timely and

accurate manner when and how the Data Breach occurred.

104. Halliburton owed these duties of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

105. Halliburton tortiously failed to take the precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Halliburton's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

### G. Plaintiff and Class Members Suffered Common Injuries and Damages due to Halliburton's Deficient Data Security and the Resulting Data Breach.

106. Halliburton's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately caused injuries to Plaintiff and Class Members by the resulting disclosure of their Private Information to a criminal ransomware group in the Data Breach.

107. Halliburton's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to (a) closely monitor their medical statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

108. The unencrypted Private Information of Plaintiff and Class Members compromised in the Data Breach will almost certainly be published on the dark web by RansomHub within the next 90 days, at most. Unauthorized individuals with nefarious intentions will easily be able to

access Plaintiff's and Class Members' Private Information—and thousands visit RansomHub's dark web leak site each day for that purpose.

109. The ramifications of Halliburton's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

110. Plaintiff and Class Members are also at a continued risk because their Private Information remains in Halliburton's systems, which have already been shown to be susceptible to compromise and are subject to further attack so long as Halliburton fails to undertake the necessary and appropriate security and training measures to protect its employees' Private Information.

111. As a result of Halliburton's ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiff's and Class Members' Private Information ending up in criminals' possession, Plaintiff and Class Members have suffered and will continue to suffer the following injuries and damages, without limitation: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Halliburtons; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in Halliburton's possession and is subject to further unauthorized disclosures so long as Halliburton fails to undertake appropriate and adequate measures to protect the Private Information it collects and maintains.

***Present and Ongoing Risk of Identity Theft***

112. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

113. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201.

114. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the data by selling it on the internet black market to other criminals, who then utilize it to commit a variety of identity theft related crimes discussed below. Thus, unauthorized actors can, and will, now easily access and misuse Plaintiff's and Class Members' Private Information due to the Data Breach.

115. The dark web is an unindexed layer of the internet that requires special software or authentication to access. Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion. This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

116. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PHI and PII like the Private Information at issue here. The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers,

dates of birth, and medical information.

117. The unencrypted Private Information of Plaintiff and Class Members will end up published and/or for sale on the dark web because that is the *modus operandi* of RansomHub and of visitors to RansomHub's dark web leak site.

118. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members.

119. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

120. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

121. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive

financial fraud[29]:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

122. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

123. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

124. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in

[29] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[30] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 23, 2024).

the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[31]

125. Theft of PHI is gravely serious as well: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[32]

126. PHI is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.

127. "Actors buying and selling PII and PHI . . . in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[33]

128. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[34]

129. "The reality is that cybercriminals seek nefarious outcomes from a data breach,"

---

[31] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[32] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Aug. 23, 2024).

[33] DistilInfo, *70% Of Data Involved In Healthcare Breaches Increases Risk of* Fraud (Oct. 3, 2019), https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/ (last visited Aug. 23, 2024).

[34] Experian, *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, available at https://www.experian.com/assets/databreach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed Mar. 14, 2023).

and "stolen health data can be used to carry out a variety of crimes."[35]

130. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[36]

131. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

132. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals can still easily create a Fullz package and sell it at a higher price to unscrupulous operators (such as illegal and scam telemarketers) and other nefarious actors over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this

---

[35] HealthTech, *What Happens to Stolen Healthcare Data?*, Oct. 30, 2019, https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Aug. 23, 2024).

[36] Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

133. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[37]

134. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[38]

135. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

136. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

---

[37] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).
[38] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

137. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

***Loss of Time to Mitigate the Risk of Identify Theft and Fraud***

138. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

139. In the likely event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face substantial costs and time to repair the damage to their good name and credit record.

140. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

141. Plaintiff and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

142. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach,

including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

143. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Halliburton's conduct that caused the Data Breach.

***Diminished Value of Private Information***

144. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

145. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

146. Private Information can sell for as much as $363 per record according to the Infosec Institute.[40]

147. PHI is especially valuable to identity thieves. According to account monitoring

[39] *See* FTC, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).
[40] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

company LogDog, medical data sells on the dark web for $50 and up.

148. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[41]

149. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for threat actors. Consequentially, Plaintiff and Class Members have been deprived of the opportunity to use or profit from their own Private Information as they choose.

150. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

***Reasonable and Necessary Future Costs of Credit and Identify Theft Monitoring***

151. To date, Halliburton has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach. Halliburton has not offered Data Breach victims even minimal compensation like complimentary credit monitoring services, or even bothered to notify its employees about their Private Information's unauthorized exposure in the Data Breach.

[41] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

152. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the *modus operandi* of RansomHub, there is an almost-certain probability that entire batches of stolen Private Information will be placed on the black market/dark web for sale and purchase by criminals intending to utilize it for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

153. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

154. Furthermore, the Private Information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts. The Private Information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

155. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

156. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Halliburton's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Halliburton's failure to safeguard their Private Information.

***Lost Benefit of the Bargain***

157. Furthermore, Halliburton's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

158. When agreeing to provide their Private Information, which was a condition precedent to obtain employment and compensation from Halliburton, Plaintiff and Class Members, as Halliburton's current and former employees, understood and expected that they were being compensated, in part, commensurate with Halliburton's data security measures to protect the Private Information employees were required to provide.

159. In fact, Halliburton did not provide the expected and bargained-for data security. Accordingly, Plaintiff and Class Members received compensation for their employment that was of a lesser value than what they reasonably expected to receive under the bargains struck with Halliburton.

## V. PLAINTIFF'S EXPERIENCE

160. Plaintiff Daniel Jandres is a former employee of Halliburton, having been employed with Halliburton from 2019 to August of 2024.

161. As a material condition of employment, Plaintiff was required to provide Halliburton with his Private Information, including his full name, date of birth, address, Social Security number, identification documents, bank account number and other financial information, health insurance information, and other sensitive PII and PHI.

162. Upon information and belief, when the Data Breach occurred, Halliburton retained Plaintiff's Private Information in its network system(s), and Plaintiff's Private Information was compromised in Halliburton's Data Breach.

163. Plaintiff greatly values his privacy and is very careful about sharing his sensitive

Private Information. Plaintiff diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

164. Plaintiff would not have provided his Private Information to Halliburton had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

165. Plaintiff learned about the Data Breach through a friend and current Halliburton employee. The current employee additionally informed Plaintiff that approximately one week after discovering the Data Breach Halliburton still had not resolved it, and many if not most of its internal programs and systems remained down and inaccessible.

166. There are also reports that the Data Breach and its aftermath have caused delays in Halliburton's payroll functions.

167. Plaintiff has already made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now anticipates having to monitor his financial and credit statements multiple times a week and spend hours dealing with the Data Breach, valuable time he would otherwise be spending on other activities.

168. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach, including the substantial, imminent, and concrete risk of identity theft he now faces due to his Private Information's unauthorized disclosure. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

169. The risk of identity theft is impending and has materialized, as Ransomware has already threatened to publish Plaintiff's and putative Class Members' Private Information on the dark web.

170. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Halliburton has still not fully informed him of key details about the Data Breach's occurrence or the information stolen. Plaintiff especially fears that his personal financial security is at substantial risk.

171. Other than this Data Breach, Plaintiff is not aware of ever being part of a data breach or similar cybersecurity incident involving his Private Information and is concerned that it has now been exposed to bad actors.

## VI. CLASS ALLEGATIONS

172. Plaintiff bring this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3).

173. Plaintiff proposes the following Class definition, subject to amendment based on information obtained through discovery:

> All individuals in the United States whose Private Information was compromised in Halliburton's Data Breach (the "Class").

174. Excluded from the Class are Halliburton's officers and directors; any entity in which Halliburton has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Halliburton. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

175. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

176. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

177. This action satisfies the requirements for a class action under Rule 23(a)(1)–(3) and Rule 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

178. **Numerosity, Rule 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Private Information of approximately at least thousands of customers and/or employees of Halliburton was compromised in the Data Breach. Such information is or will be readily ascertainable from Halliburton's records.

179. **Commonality, Rule 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Halliburton unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Halliburton failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Halliburton's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

d. Whether Halliburton's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether hackers obtained Plaintiff's and Class Members' Private Information in the Data Breach;

f. Whether Halliburton knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Halliburton's misconduct;

h. Whether Halliburton breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and Class Members; and

i. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

180. **Typicality, Rule 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

181. **Adequacy, Rule 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating data breach class actions.

182. **Predominance, Rule 23(b)(3):** Halliburton has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was stored on the same computer systems and unlawfully exposed in the same way.

The common issues arising from Halliburton's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

183. **Superiority, Rule 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions.

b. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

c. When the liability of Halliburton has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Halliburton to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

d. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including

those incurred by Halliburton, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Halliburton.

184. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Halliburton's current and former employees, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Halliburton's records, such that direct notice to the Class Members would be appropriate.

185. In addition, Halliburton has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

186. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Halliburton failed to timely and adequately notify the public of the Data Breach;

b. Whether Halliburton owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Halliburton's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Halliburton's failure to institute adequate protective security measures amounted to negligence;

e. Whether Halliburton failed to take commercially reasonable steps to safeguard customers' and employees' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

187. Finally, all members of the proposed Class are readily ascertainable. Halliburton has or will have access to Class Members' names and addresses affected by the Data Breach.

## VII. CAUSES OF ACTION

### COUNT I: NEGLIGENCE
**(On Behalf of Plaintiff and the Class against HES and Halliburton Company)**

188. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 187 above as if fully set forth herein.

189. Halliburton Company and HES required Plaintiff and Class Members to submit private, confidential Private Information to HES and Halliburton Company as a condition of receiving employment and compensation from Halliburton.

190. Plaintiff and Class Members provided their Private Information to HES and Halliburton Company including their names, Social Security numbers, dates of birth, identification documents, bank account and financial information, health insurance information, and other sensitive PHI and PII.

191. HES and Halliburton Company had full knowledge of the sensitivity of the Private Information to which they were entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized

persons.

192. HES and Halliburton Company each had a joint and several duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the Private Information collected from them.

193. Plaintiff and Class Members were the foreseeable victims of any inadequate data safety and security practices by HES or Halliburton Company.

194. Plaintiff and the Class Members had no ability to protect their Private Information in HES's and Halliburton Company's possession.

195. By collecting, transmitting, and storing Plaintiff's and Class Members' Private Information in their shared, cloud-based network servers and systems, HES and Halliburton Company each had a joint and several duty of care to use reasonable means to secure and safeguard the Private Information, to prevent its unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. HES's and Halliburton Company's duty included the responsibilities to implement processes by which they could detect and identify malicious activity or unauthorized access on their networks or servers.

196. HES and Halliburton Company each owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information. This duty included the responsibility to train employees to recognize and prevent attempts to gain initial unauthorized access through common techniques like phishing.

197. HES and Halliburton Company's duty of care to use reasonable security measures arose because of the special relationship that existed between them and their employees, which is

recognized by laws and regulations including but not limited to the FTC Act, as well as the common law. HES and Halliburton Company were able to ensure that their network systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach, yet they failed to do so.

198. In addition, HES and Halliburton Company each had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

199. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, HES and Halliburton Company each had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

200. HES and Halliburton Company each breached their duty to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

201. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly and indirectly caused by Halliburton's violation of the FTC Act.

202. Plaintiff and Class Members are within the class of persons the FTC Act is intended to protect.

203. The type of harm that resulted from the Data Breach was the type of harm the FTC Act is intended to guard against.

204. Halliburton's failure to comply with the FTC Act constitutes negligence *per se.*

205. HES and Halliburton Company's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential Private Information in its possession arose not only

because of the statutes and regulations described above, but also because HES and Halliburton Company are bound by industry standards to reasonably protect such Private Information.

206. HES and Halliburton Company each breached their duties of care, and were grossly negligent, by acts of omission or commission, by failing to use reasonable measures or even minimally reasonable measures, to protect the Plaintiff's and Class Members' Private Information from unauthorized disclosure in this Data Breach. The specific negligent acts and omissions committed by both HES and Halliburton Company include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Maintaining and/or transmitting Plaintiff's and Class Members' Private Information in unencrypted and identifiable form;

c. Failing to implement data security measures, like adequate MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to network servers and systems;

d. Failing to adequately train employees on proper cybersecurity protocols;

e. Failing to adequately monitor the security of their networks and systems;

f. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

g. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

207. But for HES's and Halliburton Company's wrongful and negligent breaches of their duties owed to Plaintiff and Class Members, their Private Information would not have been compromised because the malicious activity would have been identified and stopped before RansomHub had a chance to inventory HES and Halliburton Company's digital assets, stage them,

and then exfiltrate them.

208. It was foreseeable that HES's and Halliburton Company's failures to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in Halliburton's industries.

209. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information cause them one or more types of injuries.

210. As a direct and proximate result of HES's and Halliburton Company's negligence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their Private Information's disclosure to cybercriminals; and (g) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in HES and Halliburton Company's possession and is subject to further unauthorized disclosures so long as HES and Halliburton Company fail to undertake appropriate and adequate measures to protect it.

211. Plaintiff and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, in an amount to be proven at trial.

212. Plaintiff and Class Members are also entitled to injunctive relief requiring HES and Halliburton Company to (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide

adequate and lifetime credit monitoring to all Class Members.

**COUNT II: BREACH OF IMPLIED CONTRACT**
**(On Behalf of Plaintiff and the Class against HES and Halliburton Company)**

213. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 187 above as if fully set forth herein.

214. Halliburton required Plaintiff and Class Members to provide and entrust their Private Information to HES and Halliburton Company as a condition of receiving employment and compensation.

215. When Plaintiff and Class Members provided their Private Information to HES and Halliburton Company, they entered into implied contracts with HES and Halliburton Company pursuant to which HES and Halliburton Company each agreed and were bound to safeguard and protect such Private Information from unauthorized access, use, and disclosure.

216. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with HES and Halliburton Company when they agreed to provide their Private Information to HES and Halliburton Company.

217. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with HES and Halliburton Company included HES's and Halliburton Company's promises to protect Private Information they collected from Plaintiff and Class Members, or created on their own, from unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on HES's and Halliburton Company's promises.

218. Under the implied contracts, HES and Halliburton Company promised and were each obligated to (a) provide and/or facilitate Plaintiff's and Class Members' employment and compensation, and (b) use reasonable data security measures to protect Plaintiff's and Class Members' Private Information provided or created as a condition of that employment and

compensation. In exchange, Plaintiff and Class Members agreed to provide HES and Halliburton Company with their Private Information and labor, and that the compensation Plaintiff and Class Members would receive for such labor took into account HES's and Halliburton Company's reasonable expenses toward employee data privacy.

219. Both the provision of employment and attendant compensation, and the protection of Plaintiff's and Class Members' Private Information, were material aspects of these implied contracts with HES and Halliburton Company.

220. HES's and Halliburton Company's implied contracts for employment—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including HES and Halliburton Company's Code of Business Conduct and Privacy Statement, as described *supra*.

221. HES and Halliburton Company solicited and invited Plaintiff and Class Members to provide their Private Information as part of HES's and Halliburton Company's respective regular business practices. Plaintiff and Class Members accepted HES's and Halliburton Company's offers and provided their Private Information to HES and Halliburton Company.

222. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that HES's and Halliburton Company's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

223. Plaintiff and Class Members, who partnered or contracted with HES and Halliburton Company for employment and provided their Private Information to HES and Halliburton Company, reasonably believed and expected that HES and Halliburton Company would adequately employ adequate data security to protect the Private Information they received

and used. Both HES and Halliburton Company failed to do so.

224. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their Private Information to HES and Halliburton Company and agreed HES and Halliburton Company would receive labor for, amongst other things, the protection of their Private Information.

225. Plaintiff and Class Members performed their obligations under the contracts when they provided their labor and Private Information to HES and Halliburton Company.

226. HES and Halliburton Company each materially breached their joint and several contractual obligations to protect Plaintiff's and Class Members' Private Information by failing to encrypt files containing Private Information or implement even minimally reasonable logging and monitoring systems, among other safeguards, and thus causing the disclosure of Plaintiff's and Class Members' data to a notorious ransomware group bent on identity theft, fraud, and extortion.

227. HES and Halliburton Company each materially breached the terms of their implied contracts, including, but not limited to, by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, or by failing to otherwise protect Plaintiff's and Class Members' Private Information from unauthorized breach and disclosure, as set forth *supra*.

228. The Data Breach was a reasonably foreseeable consequence of HES's and Halliburton Company's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

229. As a result of HES's and Halliburton Company's failures to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with HES or Halliburton Company, and instead received compensation for

employment of a diminished value compared to that contemplated and agreed-to. Plaintiff and Class Members were therefore damaged in an amount at least equal to the higher payments they should have received for their employment given the increased risk such employment posed to their Private Information in HES and Halliburton Company's care.

230. Had HES or Halliburton Company disclosed that their data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have contracted for employment with HES or Halliburton Company.

231. Plaintiff and Class Members would not have provided and entrusted their Private Information to HES and Halliburton Company in the absence of the implied contracts between them and HES and Halliburton Company.

232. As a direct and proximate result of HES's and Halliburton Company's breaches of their implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with HES and Halliburton Company.

233. Plaintiff and Class Members, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

## COUNT III: INVASION OF PRIVACY
**(On Behalf of Plaintiff and the Class against HES and Halliburton Company)**

234. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 187 above as if fully set forth herein.

235. Plaintiff and Class Members had a legitimate expectation of privacy to their Private

Information and were entitled to HES and Halliburton Company's protection of this Private Information in their possession against disclosure to unauthorized third parties.

236. HES and Halliburton Company owed a duty to their employees, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

237. HES and Halliburton Company failed to protect Plaintiff's and Class Members' Private Information and instead exposed it to unauthorized persons, a notorious ransomware group, which will almost certainly make the Private Information publicly available, including through publishing the data on its dark web leak site, where cybercriminals go to find their next identity theft and extortion victims.

238. HES and Halliburton Company allowed unauthorized third parties access to and examination of the Private Information of Plaintiff and Class Members, by way of HES and Halliburton Company's failure to protect the Private Information.

239. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

240. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to HES and Halliburton Company as a condition of employment and compensation, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

241. Subsequent to the intrusion, HES and Halliburton Company permitted Plaintiff's

and Class Members' data to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

242. The Data Breach constitutes an intentional or reckless interference by HES and Halliburton Company with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

243. HES and Halliburton Company acted in concert and with knowing states of mind when they permitted the Data Breach to occur, because they had actual knowledge that their information security practices were inadequate and insufficient.

244. HES and Halliburton Company acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to their systems containing Plaintiff's and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

245. HES and Halliburton Company were aware of the potential of a data breach and failed to adequately safeguard their network systems or implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' Private Information.

246. Because HES and Halliburton Company each acted with this knowing state of mind, both had notice and knew of the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

247. As a direct and proximate result of HES's and Halliburton Company's joint acts and omissions set forth above, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages as set forth herein, including, without limitation, (a) invasion of privacy; (b) lost or

diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which remains in HES and Halliburton Company's possession in unencrypted form and subject to further unauthorized disclosures, so long as HES and Halliburton Company fail to undertake appropriate and adequate measures to protect it.

248. Unless and until enjoined, and restrained by order of this Court, HES and Halliburton Company's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by HES and Halliburton Company can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

## COUNT IV: UNJUST ENRICHMENT
**(On Behalf of Plaintiff and the Class against HES and Halliburton Company)**

249. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 187 above as if fully set forth herein.

250. This claim is pleaded in the alternative to the claim of breach of implied contract.

251. Plaintiff and Class Members conferred direct benefits upon HES and Halliburton Company in the form of agreeing to provide their Private Information to HES and Halliburton Company, without which neither company could perform the services it provides, staff or pay employees, comply with commercial contractual obligations, or generate revenue.

252. HES and Halliburton Company appreciated or knew of these benefits they received from Plaintiff and Class Members. Under principles of equity and good conscience, HES and Halliburton Company should not be allowed to retain the full value of these benefits—specifically,

the costs they saved by failing to implement reasonable or adequate data security practices with respect to the Private Information they collected from Plaintiff and Class Members.

253. After all, HES and Halliburton Company failed to adequately protect Plaintiff's and Class Members' Private Information. And if such inadequacies were known, then Plaintiff and Class Members would never have agreed to provide their Private Information or labor to HES or Halliburton Company.

254. HES and Halliburton Company should be compelled to disgorge into a common fund, for the benefit of Plaintiff and the Class, all funds that were unlawfully or inequitably gained despite HES's and Halliburton Company's misconduct and the resulting Data Breach.

**COUNT V: DECLARATORY JUDGMENT**
**(On behalf of Plaintiff and the Class against HES and Halliburton Company)**

255. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 187 above as if fully set forth herein.

256. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary supplemental relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

257. In the fallout of the Data Breach, a controversy has arisen about HES and Halliburton Company's duties to use reasonable data security for the Private Information they collect and maintain from employees.

258. On information and belief, HES and Halliburton Company's actions were—and *still* are—inadequate and unreasonable. Plaintiff and Class Members continue to suffer injuries from the ongoing threat of fraud and identity theft due to HES and Halliburton Company's inadequate data security measures.

259. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring as follows:

a. HES and Halliburton Company owed—and continue to owe—a legal duty to use reasonable data security to secure the Private Information entrusted to them;

b. HES and Halliburton Company have a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. HES and Halliburton Company's breached, and continue to breach, their duties by failing to use reasonable measures to protect the Private Information entrusted to them from unauthorized access, use, and disclosure; and

d. HES and Halliburton Company's breaches of duties caused—and continue to cause—injuries to Plaintiff and Class Members.

260. The Court should also issue injunctive relief requiring HES and Halliburton Company to use adequate security consistent with industry standards to protect the Private Information entrusted to them.

261. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injuries and lack an adequate legal remedy if HES and/or Halliburton Company experiences a second data breach. And if a second breach occurs, Plaintiff and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted for out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiff's and Class Members' injuries.

262. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that HES and Halliburton Company could experience if an

injunction is issued.

263. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

## VIII. PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff Daniel Jandres, on behalf of himself and all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, statutory, nominal, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiff and the Class;

F. Enjoining Defendants from further deceptive practices and making untrue statements about their data security, the Data Breach, and the transmitted Private Information;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law; and

I. Awarding such further relief to which Plaintiff and the Class are entitled.

## IX. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues to triable.

Dated: September 5, 2024.

Respectfully submitted,

By: /s/ *Bruce Steckler*
Bruce W. Steckler (Texas Bar No. 785039)
**STECKLER WAYNE & LOVE PLLC**
12720 Hillcrest Road, Ste. 1045
Dallas, TX 75230
Tel: (972) 387-4040
bruce@stecklerlaw.com

Jeff Ostrow (*pro hac vice* application forthcoming)
**KOPELOWITZ OSTROW P.A.**
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

***Counsel for Plaintiff and the Putative Class***